

DATA TERMINAL EQUIPMENT

Publication number: JP2002091827 (A)

Publication date: 2002-03-29

Inventor(s): HORI YOSHIHIRO

Applicant(s): SANYO ELECTRIC CO

Classification:

- international: **G06F12/14; G06F12/00; G06F21/24; G06Q30/00; G10K15/02; G06F12/14; G06F12/00; G06F21/00; G06Q30/00; G10K15/02; (IPC1-7): G06F12/14; G06F12/00; G06F17/60**

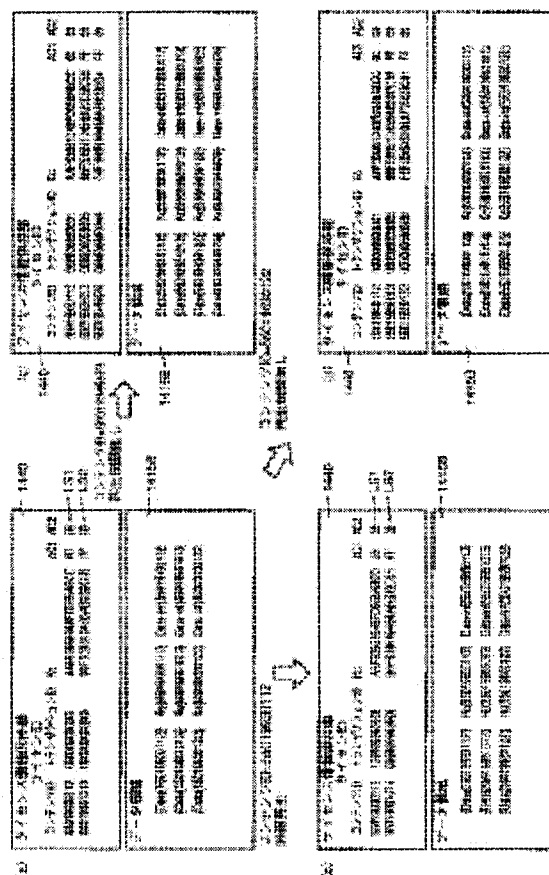
- European:

Application number: JP20000284862 20000920

Priority number(s): JP20000284862 20000920

Abstract of JP 2002091827 (A)

PROBLEM TO BE SOLVED: To provide portable terminal equipment for receiving only required enciphered contents data and/or license key or the like from a distribution server. **SOLUTION:** When the receiving request of enciphered contents data Data} Kc is inputted from a user, a portable telephone set retrieves the recording conditions of a contents ID, license key Kc, reproducing time limit information AC1, reproducing time limit and enciphered contents data Data}Kc or the like on a loaded memory card. Then, only the enciphered contents data Data}Kc and license (contents ID, license key Kc, reproducing time limit information AC1 and reproducing time limit), which are not recorded in a license area 1415A and a data area 1415B of the memory card are received from the distribution server.



Data supplied from the **esp@cenet** database — Worldwide

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2002-91827

(P2002-91827A)

(43)公開日 平成14年3月29日(2002.3.29)

| (51)Int.Cl. ⁷ | 識別記号 | F I | テームト*(参考) |
|--------------------------|-------|---------------|-------------------|
| G 0 6 F 12/14 | 3 2 0 | C 0 6 F 12/14 | 3 2 0 B 5 B 0 1 7 |
| 12/00 | 5 3 7 | 12/00 | 5 3 7 H 5 B 0 4 9 |
| 17/60 | 3 0 2 | 17/60 | 3 0 2 E 5 B 0 8 2 |

審査請求 未請求 請求項の数14 O L (全 31 頁)

(21)出願番号 特願2000-284862(P2000-284862)

(22)出願日 平成12年9月20日(2000.9.20)

(71)出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72)発明者 堀 吉宏

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74)代理人 100064746

弁理士 深見 久郎 (外3名)

Fターム(参考) 5B017 AA07 BA07 BB07 CA16

5B049 AA05 AA06 EE05 FF01 FF08

CC00

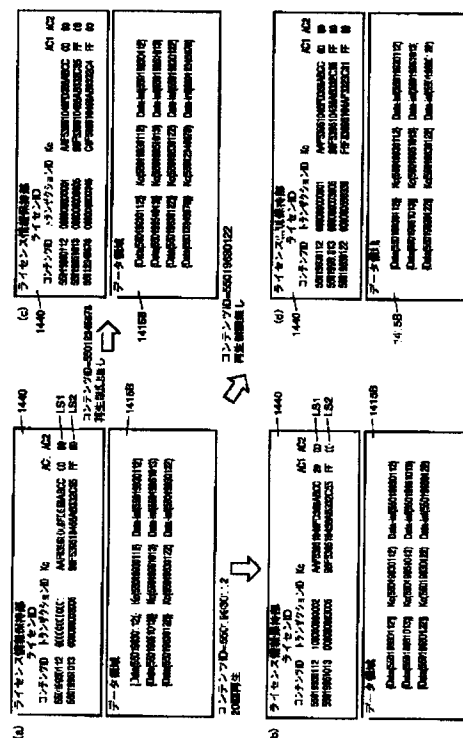
5B082 CA11

(54)【発明の名称】 データ端末装置

(57)【要約】

【課題】 必要な暗号化コンテンツデータおよび/またはライセンス鍵等のみを配信サーバから受信する携帯端末装置を提供する。

【解決手段】 携帯電話機は、ユーザから暗号化コンテンツデータ{Data}Kcの受信要求が入力されると、装着されたメモリカードにおけるコンテンツID、ライセンス鍵Kc、再生回数制限情報AC1、再生期限、および暗号化コンテンツデータ{Data}Kc等の記録状況を検索する。そして、メモリカードのライセンス領域1415A、データ領域1415Bに記録されていない暗号化コンテンツデータ{Data}Kc、およびライセンス(コンテンツID、ライセンス鍵Kc、再生回数制限情報AC1、再生期限)だけを配信サーバから受信する。



【特許請求の範囲】

【請求項1】 コンテンツデータを暗号化した暗号化コンテンツデータおよび／または前記暗号化コンテンツデータを再生するためのライセンスを配信サーバから受信して、前記暗号化コンテンツデータおよび／または前記ライセンスを記録するデータ端末装置であって、前記暗号化コンテンツデータおよび前記ライセンスを記録するデータ記録部と、

外部との通信を行なう送受信部と、

前記データ記録部とのデータ授受を制御するインタフェースと、

指示を入力するためのキー操作部と、

制御部とを備え、

前記制御部は、前記キー操作部を介して暗号化コンテンツデータの受信要求が入力されると、受信要求された暗号化コンテンツデータが前記データ記録装置に記録されているかを検索し、かつ、受信要求された暗号化コンテンツデータを再生することができるライセンスの有無を検索し、

前記暗号化コンテンツデータが前記データ記録部に記録されていないとき、および／または前記ライセンスが無いとき、前記暗号化コンテンツデータおよび／または前記ライセンスの配信を前記送受信部を介して配信サーバへ要求する、データ端末装置。

【請求項2】 前記制御部は、前記送受信部が前記配信サーバから受信した暗号化コンテンツデータのメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に、前記暗号化コンテンツデータおよび／または前記ライセンスの検索を行なう、請求項1に記載のデータ端末装置。

【請求項3】 前記受信要求する暗号化コンテンツデータの決定は、前記メニュー情報に含まれた暗号化コンテンツデータを特定するためのコンテンツIDが選択されることによって行なわれ、

前記制御部は、前記選択されたコンテンツIDに基づいて前記暗号化コンテンツデータおよび／または前記ライセンスの検索を行なう、請求項2に記載のデータ端末装置。

【請求項4】 前記制御部は、前記暗号化コンテンツデータの検索を行ない、前記暗号化コンテンツデータが前記データ記録部に記録されていないとき、前記暗号化コンテンツデータの配信を前記送受信部を介して前記配信サーバへ要求する、請求項1から請求項3のいずれか1項に記載のデータ端末装置。

【請求項5】 前記制御部は、前記暗号化コンテンツデータが前記データ記録装置に記録されているとき、前記ライセンスの検索を行なう、請求項4に記載のデータ端末装置。

【請求項6】 前記ライセンスは、少なくとも前記暗号化コンテンツデータを復号するためのライセンス鍵と、

前記暗号化コンテンツデータの再生を制限する再生制限情報とから成り、

前記制御部は、受信要求された暗号化コンテンツデータが前記データ記録部に記録されており、前記ライセンス鍵および前記再生制限情報が前記データ記録部に記録されていないとき、前記ライセンスが無いと判断する、請求項1に記載のデータ端末装置。

【請求項7】 前記ライセンスは、少なくとも前記暗号化コンテンツデータを復号するためのライセンス鍵と、前記暗号化コンテンツデータの再生を制限する再生制限情報とから成り、

前記制御部は、受信要求された暗号化コンテンツデータおよびその暗号化コンテンツデータを復号するためのライセンス鍵が前記データ記録部に記録されており、前記暗号化コンテンツデータの再生が前記再生制限情報によって制限されているとき、前記ライセンスが無いと判断する、請求項1に記載のデータ端末装置。

【請求項8】 前記制御部は、前記キー操作部から入力された変更後の再生制限情報を前記ライセンスの購入条件として前記コンテンツIDとともに前記送受信部を介して前記配信サーバへ送信する、請求項7に記載のデータ端末装置。

【請求項9】 表示部をさらに備え、

前記制御部は、前記メニュー情報を前記表示部に表示し、ユーザが前記表示部に表示された前記メニュー情報に基づいて前記コンテンツIDを選択するための情報をキー操作部を介して入力することによって、前記コンテンツIDを取得する、請求項3に記載のデータ端末装置。

【請求項10】 前記メニュー情報は、他の画面へ移行するための移行情報を含む複数の画面から構成され、前記表示部は、前記移行情報を入力するための入力部を含み、

前記制御部は、前記入力部から前記移行情報が入力されると、前記移行情報に基づいて決定される他の画面を前記表示部に表示する、請求項9に記載のデータ端末装置。

【請求項11】 前記制御部は、前記ライセンスの購入条件と、前記インタフェースを介して取得した前記データ記録部の認証データおよび前記コンテンツIDとを前記送受信部を介して前記配信サーバへ送信し、前記配信サーバにおいて前記認証データが認証された場合のみ、前記ライセンスを受信する、請求項1から請求項10のいずれか1項に記載のデータ端末装置。

【請求項12】 前記ライセンスに従って前記暗号化コンテンツデータを再生するデータ再生部をさらに備え、前記制御部は、前記キー操作部を介して暗号化コンテンツデータの再生要求が入力されると、前記暗号化コンテンツデータに対する前記ライセンスのうち少なくとも前記データ再生部に必要な情報と前記暗号化コンテンツデ

ータとを前記データ記録部から前記インタフェースを介して受取り、その受取った暗号化コンテンツデータおよび前記必要な情報を前記データ再生部に与える、請求項1から請求項11のいずれか1項に記載のデータ端末装置。

【請求項13】 前記バスに接続され、前記データ記録部に対する認証データを保持する認証データ保持部をさらに備え、

暗号化コンテンツデータの再生時、

前記制御部は、前記認証データが前記データ記録部において認証された場合のみ前記暗号化コンテンツデータに対する前記ライセンスのうち少なくとも前記データ再生部に必要な情報を前記データ記録部から前記インタフェースを介して受取り、その受取った暗号化コンテンツデータおよび前記必要な情報を前記データ再生部に与える、請求項12に記載のデータ端末装置。

【請求項14】 前記データ記録部は、着脱可能なデータ記録装置である、請求項1から請求項13のいずれか1項に記載のデータ端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）につい

ては、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモ리카ードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモ리카ードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモ리카ードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモ리카ードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモ리카ード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモ리카ード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモ리카ードに送信する。そして、メモ리카ードは、受信したライセンス鍵と暗号化コンテンツデータをメモ리카ードに記録する。

【0012】そして、メモ리카ードに記録した暗号化コンテンツデータを再生するときは、メモ리카ードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモ리카ードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータを配信サーバから受信するとき、携帯電話機は、暗号化コンテンツデータとともに暗号化コンテンツデータを復号するライセンス鍵、および暗号化コンテンツデータの再生回数、再生期限等を設定した購入条件を配信サーバから受信し、メモリカードに記録する。

【0015】また、携帯電話機は、暗号化コンテンツデータを再生するとき、暗号化コンテンツデータの再生が受信した再生回数、再生期限等によって制限されないときに暗号化コンテンツデータを再生する。

【0016】さらに、携帯電話機は、配信サーバ以外から暗号化コンテンツデータのみを受信し、メモリカードに記録する場合もある。

【0017】したがって、暗号化コンテンツデータがメモリカードに記録されているが、ライセンス鍵がメモリカードに記録されていない場合、暗号化コンテンツデータおよびライセンス鍵がメモリカードに記録されているが、再生回数、再生期限等によって暗号化コンテンツデータの再生が制限される場合、および暗号化コンテンツデータおよびライセンス鍵がメモリカードに記録されていない場合等が想定される。

【0018】かかる場合に、ユーザから暗号化コンテンツデータの配信要求がされた場合、直ちに配信サーバへ暗号化コンテンツデータおよびライセンス鍵等の配信を要求したのでは、同じ暗号化コンテンツデータおよびライセンス鍵を配信サーバから受信することになり、同じ暗号化コンテンツデータに対して料金を複数回支払うという問題が生じる。

【0019】また、暗号化コンテンツデータを配信サーバから受信するために不要な時間を必要とするという問題もある。

【0020】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、必要な暗号化コンテンツデータおよび／またはライセンス鍵等のみを配信サーバから受信するデータ端末装置を提供することである。

【0021】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび／または暗号化コンテンツデータを再生するためのライセンスを配信サーバから受信して、暗号化コンテンツデータおよび／またはライセンスを記録するデータ端末装置であって、暗号化コンテンツデータおよびライセンスを記録するデータ記録部と、外部との通信を行なう送受信部と、データ記録

部とのデータ授受を制御するインタフェースと、指示を入力するためのキー操作部と、制御部とを備え、制御部は、キー操作部を介して暗号化コンテンツデータの受信要求が入力されると、受信要求された暗号化コンテンツデータがデータ記録部に記録されているかを検索し、かつ、受信要求された暗号化コンテンツデータを再生するためのライセンスの有無を検索し、暗号化コンテンツデータがデータ記録部に記録されていないとき、および／またはライセンスが無いとき、暗号化コンテンツデータおよび／またはライセンスの配信を送受信部を介して配信サーバへ要求する。

【0022】この発明によるデータ端末装置においては、ユーザから暗号化コンテンツデータの受信要求がキー操作部を介して入力されると、制御部は、受信要求がなされた暗号化コンテンツデータおよび／またはライセンスがデータ記録部に記録されているか否かを検索し、データ記録部に記録されていない暗号化コンテンツデータおよび／またはライセンスの配信を配信サーバへ要求する。つまり、データ端末装置は、データ記録部における暗号化コンテンツデータおよびライセンスの記録状況に応じて必要な暗号化コンテンツデータおよびライセンスだけを配信サーバから受信し、かつ、データ記録部に記録する。

【0023】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよびライセンスの重複記録を防止できる。

【0024】また、この発明によれば、ライセンスを重複して受信することによる無駄な料金を配信サーバへ支払うことを防止できる。

【0025】さらに、この発明によれば、暗号化コンテンツデータを重複して受信することによって無駄な時間が発生するのを防止できる。

【0026】好ましくは、データ端末装置の制御部は、送受信部が配信サーバから受信した暗号化コンテンツデータのメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に、暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【0027】データ端末装置は、配信サーバから受信したメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【0028】したがって、この発明によれば、受信要求された暗号化コンテンツデータおよびライセンスがデータ記録部に記録されているか否かを正確に判断できる。

【0029】好ましくは、受信要求する暗号化コンテンツデータの決定は、メニュー情報に含まれた暗号化コンテンツデータを特定するためのコンテンツIDが選択されることによって行なわれ、制御部は、選択されたコンテンツIDに基づいて暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【0030】ユーザは、暗号化コンテンツデータのコンテンツIDを特定することによって受信要求する暗号化コンテンツデータを選択する。そうすると、データ端末装置の制御部は、選択された暗号化コンテンツデータのコンテンツIDを抽出し、その抽出したコンテンツIDに基づいて、暗号化コンテンツデータおよび／またはライセンスがデータ記録部に記録されているか否かを検索する。

【0031】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよび／またはライセンスの検索を正確に行なうことができる。

【0032】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータの検索を行ない、暗号化コンテンツデータがデータ記録部に記録されていないとき、暗号化コンテンツデータの配信を送受信部を介して配信サーバへ要求する。

【0033】データ端末装置の制御部は、コンテンツIDを用いてデータ記録部における暗号化コンテンツデータの検索を行ない、暗号化コンテンツデータがデータ記録部に記録されていないとき、データ記録部におけるライセンスの検索を行なうわずに暗号化コンテンツデータおよびライセンスの配信を配信サーバへ要求する。

【0034】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよびライセンスの記録状況を迅速に検索し、その記録状況に応じて必要な暗号化コンテンツデータおよびライセンスを配信サーバから受信できる。

【0035】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータがデータ記録部に記録されているとき、ライセンスの検索を行なう。

【0036】データ端末装置の制御部は、暗号化コンテンツデータがデータ記録部に記録されていないことを確認した後に、ライセンスの検索を行なう。

【0037】したがって、この発明によれば、必要な検索のみを行なうことによって検索時間を短縮し、かつ、正確な検索を行なうことができる。

【0038】好ましくは、ライセンスは、少なくとも暗号化コンテンツデータを復号するためのライセンス鍵と、暗号化コンテンツデータの再生を制限する再生制限情報とから成り、制御部は、受信要求された暗号化コンテンツデータがデータ記録装置に記録されており、ライセンス鍵および再生制限情報がデータ記録部に記録されていないとき、ライセンスが無いと判断する。

【0039】ライセンスを構成するライセンス鍵および再生制限情報がデータ記録部に記録されていないとき、データ端末装置の制御部は、受信要求された暗号化コンテンツデータのライセンスが存在しないと判断する。

【0040】したがって、この発明によれば、データ記録部に暗号化コンテンツデータのみが記録されているとき、ライセンス鍵および再生制限情報を配信サーバから

受信することができる。

【0041】好ましくは、ライセンスは、少なくとも暗号化コンテンツデータを復号するためのライセンス鍵と、暗号化コンテンツデータの再生を制限する再生制限情報とから成り、制御部は、受信要求された暗号化コンテンツデータおよびその暗号化コンテンツデータを復号するためのライセンス鍵がデータ記録部に記録されており、暗号化コンテンツデータの再生が再生制限情報によって制限されているとき、ライセンスが無いと判断する。

【0042】ライセンスを構成する再生制限情報のみがデータ記録部に記録されていないとき、データ端末装置の制御部は、受信要求された暗号化コンテンツデータのライセンスが存在しないと判断する。

【0043】したがって、この発明によれば、再生制限情報のみがデータ記録部に記録されていないとき、再生制限情報を配信サーバから受信してライセンスを取得することができる。

【0044】好ましくは、データ端末装置の制御部は、キー操作部から入力された変更後の再生制限情報をライセンスの購入条件としてコンテンツIDとともに送受信部を介して配信サーバへ送信する。

【0045】データ端末装置の制御部は、再生制限情報のみを変更することによって暗号化コンテンツデータの購入条件が設定されると、コンテンツIDとともに設定された購入条件を配信サーバへ送信する。そして、データ端末装置は、再生制限情報を配信サーバから受信し、データ記録部に記録する。

【0046】したがって、この発明によれば、ライセンスを購入して暗号化コンテンツデータを再生し、ライセンスが無くなった場合にも新たに再生制限情報だけを配信サーバから購入することによって暗号化コンテンツデータを再生することができる。

【0047】好ましくは、データ端末装置は、表示部をさらに備え、制御部は、メニュー情報を表示部に表示し、ユーザが表示部に表示されたメニュー情報に基づいてコンテンツIDを選択するための情報をキー操作部を介して入力することによって、コンテンツIDを取得する。

【0048】配信サーバから配信されたメニュー情報は、データ端末装置の表示部に表示される。そして、ユーザは表示部に表示されたメニュー情報を見て受信を希望する暗号化コンテンツデータのコンテンツIDを選択するための情報をキー操作部から入力する。そうすると制御部は、キー操作部を介して選択されたコンテンツIDを取得する。

【0049】したがって、この発明によれば、ユーザは視覚情報に基づいて受信を希望する暗号化コンテンツデータを決定できる。また、この発明によれば、コンテンツIDを選択するための情報が入力されるので、制御部

は、選択されたコンテンツIDに基づいて、暗号化コンテンツデータおよび／またはライセンスの検索を迅速に行なうことができる。

【0050】好ましくは、メニュー情報は、他の画面へ移行するための移行情報を含む複数の画面から構成され、表示部は、移行情報を入力するための入力部を含み、制御部は、入力部から移行情報が入力されると、移行情報に基づいて決定される他の画面を表示部に表示する。

【0051】データ端末装置の表示部に表示されたメニュー情報に受信を希望する暗号化コンテンツデータが含まれていないとき、ユーザは移行情報を入力する、そうすると、データ端末装置の制御部は、次の画面に移行し、新たなメニュー情報を表示部に表示する。

【0052】したがって、この発明によれば、多くの暗号化コンテンツデータの中から受信を希望する暗号化コンテンツデータを選択できる。

【0053】好ましくは、データ端末装置の制御部は、ライセンスの購入条件と、インタフェースを介して取得したデータ記録部の認証データおよびコンテンツIDとを送受信部を介して配信サーバへ送信し、配信サーバにおいて認証データが認証された場合のみ、ライセンスを受信する。

【0054】配信サーバがデータ記録部から送られてきた認証データを認証した場合のみ、データ端末装置はライセンスを受信する。

【0055】したがって、この発明によれば、正規なデータ記録部にだけライセンスを与えることができる。その結果、暗号化コンテンツデータの保護を図ることができる。

【0056】好ましくは、データ端末装置は、ライセンスに従って暗号化コンテンツデータを再生するデータ再生部をさらに備え、制御部は、キー操作部を介して暗号化コンテンツデータの再生要求が入力されると、暗号化コンテンツデータに対するライセンスのうち少なくともデータ再生部に必要な情報と暗号化コンテンツデータとをデータ記録部からインタフェースを介して受取り、その受取った暗号化コンテンツデータおよび必要な情報をデータ再生部に与える。

【0057】暗号化コンテンツデータの再生時、制御部は、ライセンスを構成する種々の情報のうち、再生に必要な情報だけをデータ記録部から取出し、暗号化コンテンツデータと、再生に必要な情報とをデータ再生部に与える。そして、データ再生部は、必要な情報によって暗号化コンテンツデータを復号および再生する。

【0058】したがって、この発明によれば、再生に必要な情報によって暗号化コンテンツデータの再生を制限することができる。

【0059】好ましくは、データ端末装置は、データ記録部に対する認証データを保持する認証データ保持部を

さらに備え、暗号化コンテンツデータの再生時、制御部は、認証データがデータ記録部において認証された場合のみ暗号化コンテンツデータに対するライセンスのうち少なくともデータ再生部に必要な情報をデータ記録部からインタフェースを介して受取り、その受取った暗号化コンテンツデータをデータ再生部に与える。

【0060】配信サーバから受信した暗号化コンテンツデータを再生するとき、データ記録部に対するデータ端末装置の正当性が確認された場合だけ、データ端末装置はデータ記録部から暗号化コンテンツデータを受取り、暗号化コンテンツデータを再生する。

【0061】したがって、この発明によれば、正規なデータ端末装置だけが暗号化コンテンツデータを再生できる。その結果、暗号化コンテンツデータの不法なコピー等を防止して保護を図ることができる。

【0062】好ましくは、データ記録部は、データ端末装置から着脱可能なデータ記録装置である。

【0063】データ端末装置は、配信サーバから暗号化コンテンツデータおよびライセンスを受信すると、その受信した暗号化コンテンツデータおよびライセンスを着脱可能なデータ記録装置へに記録する。

【0064】したがって、この発明によれば、複数のデータ記録装置に暗号化コンテンツデータおよび／またはライセンスを記録することができる。

【0065】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0066】図1は、本発明による携帯端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0067】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても適用することが可能なものである。

【0068】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20で

ある携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【0069】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

【0070】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0071】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0072】以下では、このようなライセンスサーバ10と配信キャリア20と併せて、配信サーバ30と総称することとする。

【0073】また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0074】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0075】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0076】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0077】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生でき

るデータ再生端末を携帯電話機とも言う。以下同じ））に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0078】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0079】まず、配信サーバ30より配信されるデータについて説明する。Dataは、音楽データ等のコンテンツデータである。コンテンツデータDataには、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ{Data}Kcがこの形式で配信サーバ30より携帯電話ユーザに配布される。

【0080】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0081】さらに、配信サーバ30からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Data-infが配布される。また、配信サーバ30からの暗号化コンテンツデータおよびライセンス鍵等の配信を特定するための管理コードであるトランザクションIDが配信サーバ30と携帯電話機100との間でやり取りされる。さらに、ライセンス情報としては、コンテンツデータDataを識別するためのコードであるコンテンツIDおよびライセンスの発行を特定できる管理コードであるライセンスIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード）のアクセスに対する制限に関する情報であるアクセス制限情報AC1およびデータ再生端末における制御情報である再生期限AC2等が存在する。以後、ライセンス鍵KcとコンテンツIDとライセンスIDと再生回数期限AC1と再生期限AC2とを併せて、ライセンスと総称することとする。

【0082】図3は、図1に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【0083】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストCRL(Class Revocation List)の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0084】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機およびメモリカードのクラスをリストアップした禁止クラスリス

トデータCRLが含まれる。

【0085】禁止クラスリストデータCRLは、配信サーバ30内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際の日時を基準として、携帯電話機から受取った禁止クラスリストの更新の有無を判断し、更新されていないとき、更新された禁止クラスリストを携帯電話機に配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データCRL_{dat}を配信サーバ30側より発生して、これに応じてメモリカード内の禁止クラスリストCRLが書替えられる構成とするも可能である。また、禁止クラスリストのバージョンについては、CRL_{ver}をメモリカード側より出力し、これを配信サーバ30側で確認することによってバージョン管理を実行する。差分データCRL_{dat}には新たなバージョンの情報も含まれる。

【0086】このように、禁止クラスリストCRLを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードへのライセンス鍵の供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行えなくなる。

【0087】このように、メモリカード内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストCRLの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール(Tamper Resistance Module)に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【0088】携帯電話機およびメモリカードには固有の公開暗号鍵K_{Ppn}およびK_{Pmci}がそれぞれ設けられ、公開暗号鍵K_{Ppn}およびK_{Pmci}は携帯電話機に固有の秘密復号鍵K_pおよびメモリカード固有の秘密復号鍵K_{mci}によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【0089】また、データ再生端末(携帯電話機)およびメモリカードのクラス証明書として、C_{rtn}およびC_{mci}がそれぞれ設けられる。これらのクラス証明

書は、メモリカードおよびコンテンツ再生端末のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【0090】これらのメモリカードおよびコンテンツ再生端末固有の公開暗号鍵およびクラス証明書は、認証データ{K_{Pmci}／／C_{mci}}K_{Pma}および{K_{Ppn}／／C_{rtn}}K_{Pma}の形式で、出荷時にメモリカードおよびデータ再生端末(携帯電話機)にそれぞれ記録される。後ほど詳細に説明するが、K_{Pma}は配信システム全体で共通の公開認証鍵である。

【0091】図4は、図1に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【0092】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ30、携帯電話機100、メモリカード110において生成される共通鍵K_{s1}～K_{s3}が用いられる。

【0093】ここで、共通鍵K_{s1}～K_{s3}は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵K_{s1}～K_{s3}を「セッションキー」とも呼ぶこととする。

【0094】これらのセッションキーK_{s1}～K_{s3}は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーK_{s1}は、配信サーバによって配信セッションごとに発生される。セッションキーK_{s2}は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーK_{s3}は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0095】また、メモリカード110内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵K_{Pm}と、公開暗号鍵K_{Pm}で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵K_mが存在する。

【0096】図5は、図1に示したライセンスサーバ10の構成を示す概略ブロック図である。

【0097】ライセンスサーバ10は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための情報データベース

304と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストCRLを管理するCRLデータベース306と、情報データベースに保持されたコンテンツデータのメニューを保持するメニューデータベース307と、コンテンツデータおよびライセンス鍵等の配信を特定するトランザクションIDを保持する配信記録データベース308と、情報データベース304、課金データベース302、CRLデータベース306、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0098】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ{Kp mci // Cmci} Kpmaを復号するための公開認証鍵を保持する認証鍵保持部313と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ{Kp mci // Cmci} Kpmaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵Kpmaによって復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られた公開暗号鍵Kp mciを用いて暗号化して、バスBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0099】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよび再生期限AC2を、復号処理部320によって得られたメモリカード固有の公開暗号鍵Kp mによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号化処理部328とを含む。

【0100】ライセンスサーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0101】図6は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0102】携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド

信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのバスBS2と、バスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106とを含む。

【0103】携帯電話機100は、さらに、外部からの指示を携帯電話機100に与えるためのキー操作部1108と、コントローラ1106等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ1110と、通常の通話動作において、データベースBS2を介して与えられる受信データに基づいて音声再生するための音声再生部1112とを含む。

【0104】携帯電話機100は、さらに、音声再生部1112の出力をデジタル信号からアナログ信号に変換するDA変換器1113と、DA変換器1113の出力を外部出力装置等へ出力するための端子1114とを含む。

【0105】携帯電話機100は、さらに、通常の通話動作において、携帯電話機100のユーザが話した音声信号を入力するマイク1115と、マイク1115からの音声信号をアナログ信号からデジタル信号に変換するAD変換器1116と、AD変換器1116からのデジタル信号を所定の方式に従って符号化してバスBS2へ与える音声符号化部1117とを含む。

【0106】携帯電話機100は、さらに、配信サーバ30からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード110と、メモリカード110とバスBS2との間のデータの授受を制御するためのメモリインタフェース1200とを含む。

【0107】携帯電話機100は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵Kp p1およびクラス証明書C r t f1を公開復号鍵Kpmaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kp p1 // C r t f1} Kpmaを保持する認証データ保持部1202を含む。ここで、携帯電話機（データ端末装置）100のクラスnは、n=1であるとする。

【0108】携帯電話機100は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるKp1を保持するKp1保持部1204と、バスBS2から受けたデータをKp1によって復号しメモリカード110によって発生されたセッションキーKs2を得る復号処理部1206とを含む。

【0109】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセ

セッションキー発生部1210と、発生されたセッションキーKs3を復号処理部1206によって得られたセッションキーKs2によって暗号化しバスBS2に出力する暗号化処理部1208とを含む。

【0110】携帯電話機100は、さらに、バスBS2上のデータをセッションキーKs3によって復号して出力する復号処理部1212とを含む。

【0111】携帯電話機100は、さらに、バスBS2より暗号化コンテンツデータ{Data}Kcを受けて、復号処理部1212より取得したライセンス鍵Kcによって復号しコンテンツデータを出力する復号処理部1214と、復号処理部1214の出力を受けてコンテンツデータを再生するための音楽再生部1216と、音楽再生部1216の出力をデジタル信号からアナログ信号に変換するDA変換器1218と、DA変換器1113とDA変換器1218との出力を受けて、動作モードに応じて選択的に端子1114または端子1220から出力するためのスイッチ1222と、スイッチ1222の出力を受けて、ヘッドホン130と接続するための接続端子1224とを含む。

【0112】なお、図6においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【0113】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0114】図7は、メモリカード110の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、KPmciおよびKmc iが設けられ、メモリカードのクラス証明書Cmciが設けられるが、メモリカード110においては、これらは自然数 $i=1$ でそれぞれ表わされるものとする。

【0115】したがって、メモリカード110は、認証データ{KPmci//Cmci}KPmaを保持する認証データ保持部1400と、メモリカードの種類ごとに設定される固有の復号鍵であるKmc1を保持するKmc1保持部1402と、メモリカードごとに固有に設定される秘密復号鍵Km1を保持するKm1保持部1421と、Km1によって復号可能な公開暗号鍵KPm1を保持するKPm1保持部1416とを含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵KPmciおよびクラス証明書Cmciを公開認証鍵KPmaで復号することでその正当性を認証できる状態に暗号化した認証データ{KPmci//Cmci}KPmaとして保持する。

【0116】このように、メモリカードという記録装置

の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0117】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1201を介して授受するインタフェース1423と、インタフェース1423との間で信号をやり取りするバスBS3と、バスBS3にインタフェース1423から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Kmc1をKmc1保持部1402から受けて、配信サーバ30が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1404と、KPma保持部1414から認証鍵KPmaを受けて、バスBS3に与えられるデータからKPmaによる復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444によって選択的に与えられるデータを暗号化してバスBS3に出力する暗号化処理部1406とを含む。

【0118】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られる公開暗号鍵KPpnもしくはKPmciによって暗号化してバスBS3に送出する暗号化処理部1410と、バスBS3よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号し、復号結果をバスBS4に送出する復号処理部1412とを含む。

【0119】メモリカード110は、さらに、バスBS3上のデータを公開暗号鍵KPm1と対をなすメモリカード110固有の秘密復号鍵Km1によって復号するための復号処理部1422と、禁止クラスリストのバージョン更新のためのデータCRL_datによって逐次更新される禁止クラスリストデータCRLをバスBS4より受けて格納するとともに、暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infをバスBS3より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1515は、禁止クラスリストCRLを記録したCRL領域1415Aと、コンテンツIDを含むHeader、暗号化コンテンツデータ{Data}Kc、および暗号化コンテンツデータの関連情報Data-infを記録したデータ領域1415Bとから成る。

【0120】メモリカード110は、さらに、復号処理部1422によって得られるライセンスを保持するため

のライセンス情報保持部1440と、バスBS3を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420を含む。

【0121】ライセンス情報保持部1440は、N個（N：自然数）のバンクを有し、各ライセンスに対応するライセンスをバンクごとに保持する。

【0122】なお、図7において、実線で囲んだ領域は、メモリカード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）である。

【0123】もちろん、メモリ1415も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図7に示したような構成とすることで、メモリ1415中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ1415中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1415を設ける必要がないので、製造コストが低減されるという利点がある。

【0124】以降では、簡単化のためアクセス制御情報AC1は再生回数の制限を行なう制御情報である再生回数のみを、再生回路制御情報AC2は再生可能な期限を規定する制御情報である再生期限のみを制限するものとし、アクセス制御情報AC1および再生回路制御情報AC2を、それぞれ、再生回数制限AC1、再生期限AC2と称するものとする。

【0125】図8を参照して、暗号化コンテンツデータ{Data}Kcと、ライセンス鍵Kc、再生回数制限AC1、および再生期限AC2等から成るライセンスとが記録されたメモリカード110における各種の状態について説明する。なお、図8においては、再生回数制限AC1に制限がない場合を「FF」で表し、再生期限AC2に制限がない場合を「00」で表している。図8の(a)は、暗号化コンテンツデータ{Data}Kcおよびライセンスがメモリカード110に記録されており、新たに暗号化コンテンツデータ{Data}Kcとライセンスとを配信サーバ30から受信する場合を示す。また、図8の(b)は、暗号化コンテンツデータ{Data}Kcおよびライセンス鍵Kcが存在し、一部、再生回数制限AC1によって暗号化コンテンツデータ{Data}Kcの再生が制限されている場合を示す。さらに、図8の(c)は、暗号化コンテンツデータ{Data}Kcとライセンスとが記録されており、一部の暗号化コンテンツデータ{Data}Kcを再生す

るライセンスが記録されていない場合を示す。

【0126】図8の(a)を参照して、コンテンツID：55019930112、55019951013、55019630122によって特定される暗号化コンテンツデータ：{Data(55019930112)}Kc(55019930112)、{Data(55019951013)}Kc(55019951013)、{Data(55019630122)}Kc(55019630122)、その暗号化コンテンツデータを復号するためのライセンス鍵：AAF53951046FD356ABCC、96F539510456AB332C55、F6F53695104AF3323C31が記録されている。また、コンテンツID：55019951013、55019630122によって特定される暗号化コンテンツデータは再生回数制限AC1および再生期限AC2が無制限であるが、コンテンツID：55019930112によって特定される暗号化コンテンツデータの再生回数制限AC1は20回、再生期限AC2は無制限である。したがって、データ領域1415Bに記録された3つの暗号化コンテンツデータ{Data}Kcに対するライセンスはライセンス情報保持部1440に記録されている。

【0127】図8の(b)を参照して、コンテンツID：55019930112、55019951013によって特定される暗号化コンテンツデータ：{Data(55019930112)}Kc(55019930112)、{Data(55019951013)}Kc(55019951013)、その暗号化コンテンツデータを復号するためのライセンス鍵：AAF53951046FD356ABCC、96F539510456AB332C55が記録されている。また、コンテンツID：55019951013によって特定される暗号化コンテンツデータは再生回数制限AC1および再生期限AC2が無制限であるが、コンテンツID：55019930112によって特定される暗号化コンテンツデータの再生回数制限AC1は0回、再生期限AC2は無制限である。したがって、データ領域1415Bに記録された2つの暗号化コンテンツデータ{Data}Kcのうち、1つの暗号化コンテンツデータはライセンスがライセンス情報保持部1440に記録されていない。

【0128】図8の(c)を参照して、コンテンツID：55019930112、55019951013によって特定される暗号化コンテンツデータ：{Data(55019930112)}Kc(55019930112)、{Data(55019951013)}Kc(55019951013)、その暗号化コンテンツデータを復号するためのライセンス鍵：AAF53951046FD356ABCC、96F539510456AB332C55が記録されている。また、コンテ

ンツID: 55019951013によって特定される暗号化コンテンツデータは再生回数制限AC1および再生期限AC2が無制限であり、コンテンツID: 55019930112によって特定される暗号化コンテンツデータの再生回数制限AC1は20回、再生期限AC2は無制限である。さらに、コンテンツID: 55019630122によって特定される暗号化コンテンツデータ: {Data (55019630122)} Kc (55019630122) はデータ領域1415Bに記録されているが、その暗号化コンテンツデータを再生するためのライセンス鍵Kc、再生回数制限AC1、および再生期限AC2から成るライセンスはライセンス情報保持部1440に記録されていない。したがって、データ領域1415Bに記録された3つの暗号化コンテンツデータ {Data} Kcのうち、1つの暗号化コンテンツデータに対するライセンスが存在しない。

【0129】図8を参照して説明したように、メモリカード110には、暗号化コンテンツデータ {Data} Kc、ライセンス鍵Kc、再生回数制限AC1、および再生期限AC2が記録されているか否かによって各種の状態が存在する。

【0130】次に、暗号化コンテンツデータ {Data} Kc、およびライセンス鍵Kc等が各種の状態で記録されたメモリカード110が携帯電話機100に装着され、携帯電話機100のユーザから暗号化コンテンツデータの受信要求がされた場合の動作について説明する。

【0131】図9～図12は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第1～第4のフローチャートである。

【0132】図9を参照して、携帯電話機100のユーザからキー操作部1108を介してコンテンツデータの配信要求がなされると、携帯電話機100は、コンテンツメニューの送信要求を配信サーバ30へ送信する（ステップS70）。配信サーバ30の配信制御部315は、通信装置350およびバスBS1を介してコンテンツメニューの送信要求を受信すると（ステップS72）、メニューデータベース307からバスBS1を介してコンテンツメニューを読み出し、その読み出したコンテンツメニューをバスBS1および通信装置350を介して携帯電話機100へ送信する（ステップS74）。携帯電話機110は、送受信部1104によってコンテンツメニューを受信し、コントローラ1106は、コンテンツメニューを表示部1110に表示する（ステップS76）。

【0133】そうすると、携帯電話機100の表示部1110には、図13に示すコンテンツメニュー60が表示される。ユーザは、コンテンツメニュー60の番号001、002、003、・・・を選択することによって

配信を希望する暗号化コンテンツデータを選択する。表示部1110には、別の画面に移行するための移行部1111が設けられている。ユーザは、表示部1110に表示されたコンテンツメニュー60中に希望する暗号化コンテンツデータが表示されていないとき、移行部1111をクリックする。移行部1111には、別の画面へ移行するためのアドレスが含まれている。

【0134】携帯電話機100のコントローラ1106は、コンテンツが選択された否かを判断し（ステップS78）、移行部1111をクリックされると、コントローラ1106は、移行部1111に含まれるアドレスを送受信部1104を介して配信サーバ30へ送信し、別の画面を送信するように要求する。そして、ステップS70～S78が繰返される。つまり、コンテンツメニューは、コンテンツメニュー60から成る複数の画面が階層的に配列されて構成されており、各画面は、ジャンルの異なる暗号化コンテンツデータ、同じジャンルであるが、他の暗号化コンテンツデータ等から成るコンテンツメニューによって構成されている。

【0135】そして、配信サーバ30から複数の画面によって送られてきたコンテンツメニューに、希望する暗号化コンテンツデータが含まれていないとき、配信動作はステップS170へ移行し、配信動作は終了する。

【0136】コンテンツメニュー60は、暗号化コンテンツデータを特定するためのコンテンツIDを含んでおり、ステップS78において暗号化コンテンツデータが選択されたとき、コンテンツメニューから選択された暗号化コンテンツデータのコンテンツIDが抽出される（ステップS80）。

【0137】そして、キー操作部1108を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される（ステップS82）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータの再生回数制限AC1、および再生期限AC2を設定して購入条件ACが入力される。

【0138】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ1106は、選択された暗号化コンテンツデータに対するコンテンツIDと同じコンテンツIDを有する暗号化コンテンツデータ {Data} Kcがメモリカード110に記録されていないかを検索する（ステップS84）。この場合、コントローラ1106は、選択された暗号化コンテンツデータに対応するコンテンツIDをメモリインタフェース1200を介してメモリカード110へ送信する。メモリカード110のコントローラ1420は、インタフェース1423およびバスBS3を介して携帯電話機100からコンテンツIDを受取り、その受取ったコンテンツIDがメモリ1415のHeader1424に含まれるコンテンツIDと一致するか否かによって、ユーザがコンテン

ツメニューから選択した暗号化コンテンツデータがメモリカード110に記録されているか否かを検索する。

【0139】この場合、メモリカード110のメモリ1415に記録されたHeader、Data-inf、および{Data}Kcを図14に示すように1つのデータ列としてハッシュ関数などを用いた署名データを併せて取扱うようにすれば、コンテンツIDの改組を防止することができる。署名の確認は、コンテンツIDの検査時に対応したものに関しても行なえば良い。

【0140】そして、コントローラ1106は、選択した暗号化コンテンツデータがメモリカード110に記録されているか否かを判断し(ステップS86)、暗号化コンテンツデータがメモリカード110に記録されていないとき、データを配信サーバ30から取得するためのフラグ“Yes”を立てる(ステップS88)。暗号化コンテンツデータがメモリカード110に記録されているとき、ライセンスの確認が行なわれる(ステップS90)。つまり、図8を参照して説明したようにライセンス鍵Kcがメモリカード110に記録されているか、再生回数制限AC1および再生期限AC2によって暗号化コンテンツデータの再生が制限されていないかによってライセンスの確認が行なわれる。ライセンスが存在しないときはステップS94へ移行する。ライセンスが存在し、暗号化コンテンツデータが再生できる場合、コントローラ1106は、「ライセンス単体購入？」を表示部1110に表示し、ライセンスだけを単体で購入するか否かの意思を確認する(ステップS92)。コントローラ1106は、ライセンスだけを購入しない旨の指示がキー操作部1108から入力されると、ステップS170へ移行し、暗号化コンテンツデータの配信動作は終了する。コントローラ1106は、ライセンスだけを単体で購入する旨の指示がキー操作部1108から入力されると、データを配信サーバ30から取得しないフラグ“No”を立てる(ステップS94)。

【0141】次に、図10を参照して、携帯電話機100は、ユーザが暗号化コンテンツデータを選択することによって抽出したコンテンツID(ステップS80参照)の指定による配信リクエストがなされる(ステップS100)。

【0142】メモリカード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ{KPMC1//Cmc1}KPmaが出力される(ステップS102)。

【0143】携帯電話機100は、メモリカード110からの認証のための認証データ{KPMC1//Cmc1}KPmaに加えて、コンテンツID、ライセンス購入条件のデータACとを配信サーバ30に対して送信する(ステップS104)。

【0144】配信サーバ30では、携帯電話機100からコンテンツID、認証データ{KPMC1//Cmc1}

1}KPma、ライセンス購入条件のデータACを受信し(ステップS106)、復号処理部312においてメモリカード110から出力された認証データを公開認証鍵KPmaで復号処理を実行する(ステップS108)。

【0145】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからの公開暗号鍵KPMC1と証明書Cmc1を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS110)。正当な認証データであると判断された場合、配信制御部315は、公開暗号鍵KPMC1および証明書Cmc1を承認し、受理する。そして、次の処理(ステップS112)へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵KPMC1および証明書Cmc1を受理しないで処理を終了する(ステップS170)。

【0146】認証の結果、正規の機器であることが認識されると、配信制御部315は、次に、メモリカード110のクラス証明書Cmc1が禁止クラスリストCRLにリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する(ステップS170)。

【0147】一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS112)。

【0148】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ30において、配信制御部315は、配信を特定するための管理コードであるトランザクションIDを生成する(ステップS113)。また、セッションキー発生部316は、配信のためのセッションキーKs1を生成する。セッションキーKs1は、復号処理部312によって得られたメモリカード110に対応する公開暗号鍵KPMC1によって、暗号化処理部318によって暗号化される(ステップS114)。

【0149】トランザクションIDおよび暗号化されたセッションキーKs1は、トランザクションID//{Ks1}Kmc1として、バスBS1および通信装置350を介して外部に出力される(ステップS116)。

【0150】携帯電話機100が、トランザクションID//{Ks1}Kmc1を受信すると(ステップS118)、メモリカード110においては、メモリインタフェース1200を介して、バスBS3に与えられた受信データを、復号処理部1404が、保持部1402に

保持されるメモリカード110固有の秘密復号鍵Kmc1により復号処理することにより、セッションキーKs1を復号し抽出する(ステップS120)。

【0151】コントローラ1420は、配信サーバ30で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対して、メモリカード110において配信動作時に生成されるセッションキーKs2の生成を指示する。

【0152】また、配信セッションにおいては、コントローラ1420は、メモリカード110内のメモリ1415に記録されている禁止クラスリストのデータCRL_datをメモリ1415から抽出してバスBS4に出力する。

【0153】暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1404より与えられるセッションキーKs1によって、切換スイッチ1444および1446の接点を順次切換えることによって与えられるセッションキーKs2、公開暗号鍵Kpm1および禁止クラスリストのデータCRL_datを1つのデータ列として暗号化して、{Ks2//Kpm1//CRL_dat} Ks1をバスBS3に出力する(ステップS122)。

【0154】バスBS3に出力された暗号化データ{Ks2//Kpm1//CRL_ver} Ks1は、バスBS3からインタフェース1423、端子1201およびメモリインタフェース1200を介して携帯電話機100に出力され、携帯電話機100から配信サーバ30に送信される(ステップS124)。

【0155】配信サーバ30は、トランザクションID//{Ks2//Kpm1//CRL_dat} Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、メモリカード110固有の公開暗号鍵Kpm1およびメモリカード110における禁止クラスリストのデータCRL_datを受理する(ステップS126)。

【0156】配信制御部315は、ステップS106で取得したコンテンツIDおよびライセンス購入条件のデータACに従って、ライセンスID、アクセス制限情報AC1および再生期限AC2を生成する(ステップS128)。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Kcを情報データベース304より取得する(ステップS130)。

【0157】配信制御部315は、生成したライセンス、すなわち、ライセンス鍵Kc、再生期限AC2、ライセンスID、コンテンツID、およびアクセス制限情報AC1を暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110固有の公開暗号鍵Kpm1によってライセンスを暗号化する(ステップS132) 図11を参照し

て、配信サーバ30において、メモリカード110から送信された禁止クラスリストのデータCRL_datが最新か否かが判断され、データCRL_datが最新と判断されたとき、ステップS134へ移行する。また、データCRL_datが最新でないときはステップS137へ移行する(ステップS133)。

【0158】データCRL_datが最新と判断されたとき、暗号化処理部328は、暗号化処理部326から出力された暗号化データ{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1をメモリカード110において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1} Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ{{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1} Ks2を通信装置350を介して携帯電話機100へ送信する(ステップS134)。

【0159】そして、携帯電話機100は、暗号化データ{{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1} Ks2を受信し(ステップS135)、バスBS2およびメモリインタフェース1200を介してメモリカード110へ送信する。メモリカード110の復号処理部1412は、暗号化データ{{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1} Ks2を端子1201およびインタフェース1423を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2によって復号し、{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1を受理する(ステップS136)。その後、ステップS146へ移行する。

【0160】一方、配信サーバ30において、CRL_datが最新でないと判断されると、配信制御部315は、バスBS1を介してCRLデータベース306から最新の禁止クラスリストのデータCRL_datを取得する(ステップS137)。

【0161】暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がバスBS1を介して供給する禁止クラスリストの最新データCRL_datとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データは、バスBS1および通信装置350を介して携帯電話機100に送信される(ステップS138)。

【0162】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行な

うことができ、データ配信システムのセキュリティを向上させることができる。

【0163】携帯電話機100は、送信された暗号化データ { {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1//CRL_dat} Ks2を受信し(ステップS140)、メモリインタフェース1200を介してメモリカード110へ出力する。メモリカード110においては、端子1201およびインタフェース1423を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキーKs2を用いてバスBS3の受信データを復号しバスBS4に出力する(ステップS142)。

【0164】この段階で、バスBS4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1と、CRL_datとが出力される(ステップS142)。コントローラ1420の指示によって受理した最新の禁止クラスリストCRL_datによってメモリ1415内の禁止クラスリストCRLが書き換えられる(ステップS144)。

【0165】ステップS134, S135, S136は、メモリカード110から送られてきた禁止クラスリストCRL_datが最新の場合のライセンス鍵Kc等のメモリカード110への配信動作であり、ステップS137, S138, S140, S142, S144は、メモリカード110から送られてきた禁止クラスリストCRL_datが最新でない場合のライセンス鍵Kc等のメモリカード110への配信動作である。このように、メモリカード110から送られてきた禁止クラスリストCRL_datが更新されているか否かを、逐一、確認し、更新されていないとき、最新の禁止クラスリストCRL_datをCRLデータベース306から取得し、メモリカード110に配信することによって、ライセンスの破られたメモリカードへの暗号化コンテンツデータ {Data} Kcの配信を防止し、かつ、ライセンスの破られた携帯電話機による暗号化コンテンツデータ {Data} Kcの再生を防止できる。

【0166】ステップS136またはステップS144の後、コントローラ1420の指示によって、暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンス(ライセンス鍵Kc、ライセンスID、コンテンツID、再生回数制限AC1および再生期限AC2)が受理される(ステップS148)。

【0167】コントローラ1420は、ライセンスをライセンス情報保持部1440に記録する(ステップS1

50)。

【0168】図12を参照して、携帯電話機100のコントローラ1106は、ステップS88およびステップS94において立てたフラグを参照し、配信サーバ30から暗号化コンテンツデータを取得するか否かを判断する。そして、暗号化コンテンツデータを配信サーバ30から取得しないとき、ステップS164へ移行し、暗号化コンテンツデータを配信サーバ30から取得するとき、ステップS154へ移行する。

【0169】暗号化コンテンツデータを配信サーバ30から取得するとき、携帯電話機100は、配信サーバ30から送られたトランザクションIDと、暗号化コンテンツデータの配信要求を配信サーバ30へ送信する(ステップS154)。

【0170】配信サーバ30は、トランザクションIDおよび暗号化コンテンツデータの配信要求を受信し(ステップS156)、情報データベース304より、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する(ステップS158)。

【0171】携帯電話機100は、{Data} Kc//Data-infを受信して、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを受理する(ステップS160)。暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infは、メモリインタフェース1200、端子1201、およびインタフェース1423を介してメモリカード110のバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infがそのままメモリ1415に記録される(ステップS162)。

【0172】そして、ステップS152において暗号化コンテンツデータを配信サーバ30から受信しないと判断されたときも含め、メモリカード110から配信サーバ30へは、トランザクションID//配信受理の通知が送信され(ステップS164)、配信サーバ30でトランザクションID//配信受理を受信すると(ステップS166)、課金データベース302への課金データの格納、およびトランザクションIDの配信記録データベース308への記録が行われて配信終了の処理が実行され(ステップS168)、全体の処理が終了する(ステップS170)。

【0173】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信してきた公開暗号鍵Kp1およびKmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kp1およびKmc1による暗号化が破られたクラス証明書リストに記

載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0174】また、配信サーバ30への暗号化コンテンツデータ {Data} Kcの配信要求時にメモリカード110における暗号化コンテンツデータ {Data} Kc、ライセンス鍵Kc、および再生回数制限AC1等の記録状況に応じて、必要な配信だけを配信サーバ30に要求することができる。その結果、無駄な配信を防止することができる。

【0175】次に、図15および図16を参照してメモリカード110に配信されたコンテンツデータの携帯電話機100における再生動作について説明する。図15を参照して、再生動作の開始とともに、携帯電話機100のユーザからキー操作部1108を介して再生指示が携帯電話機100にインプットされる（ステップS200）。そうすると、コントローラ1106は、バスBS2を介して認証データ保持部1202から認証データ {Kp1//Crtf1} Kpmaを讀出し、メモリインタフェース1200を介してメモリカード110へ認証データ {Kp1//Crtf1} Kpmaを入力する（ステップS201）。

【0176】そうすると、メモリカード110は、認証データ {Kp1//Crtf1} Kpmaを受理する（ステップS202）。そして、メモリカード110の復号処理部1408は、受理した認証データ {Kp1//Crtf1} Kpmaを、Kpma保持部1414に保持された公開認証鍵Kpmaによって復号し（ステップS203）、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ {Kp1//Crtf1} Kpmaが正規の認証データであるか否かを判断する認証処理を行なう（ステップS204）。復号できなかった場合、コントローラ1420は認証データ不受理の出力をデータBS3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する（ステップS206）。認証データが復号できた場合、コントローラ1420は、取得した証明書Crtf1がメモリ1415から讀出した禁止クラスリストデータに含まれるか否かを判断する（ステップS205）。この場合、証明書Crtf1にはIDが付与されており、コントローラ1420は、受理した証明書Crtf1のIDが禁止クラスリストデータの中に存在するか否かを判別する。証明書Crtf1が禁止クラスリストデータに含まれると判断されると、コントローラ1420は認証データ不受理の出力をデータBS3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する（ステップS206）。

【0177】ステップS204において認証データが公

開認証鍵Kpmaで復号できなかったとき、およびステップS205において受理した証明書Crtf1が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して認証データ不受理の出力を受けると、認証データ不受理のデータをディスプレイ1110に表示する（ステップS207）。

【0178】ステップS205において、証明書Crtf1が禁止クラスリストデータに含まれていないと判断されると、図16を参照して、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる（ステップS208）。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した {Ks2} Kp1をバスBS3へ出力する（ステップS209）。そうすると、コントローラ1420は、端子1201を介してメモリインタフェース1200へ {Ks2} Kp1を出力し、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して {Ks2} Kp1を取得する。そして、Kp1保持部1204は、秘密復号鍵Kp1を復号処理部1206へ出力する。

【0179】復号処理部1206は、Kp1保持部1204から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって {Ks2} Kp1を復号し、セッションキーKs2を暗号処理部1208へ出力する（ステップS210）。そうすると、セッションキー発生部1210は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1208へ出力する（ステップS211）。暗号処理部1208は、セッションキー発生部1210からのセッションキーKs3を復号処理部1206からのセッションキーKs2によって暗号化して {Ks3} Ks2を出力し、コントローラ1106は、バスBS2およびメモリインタフェース1200を介して {Ks3} Ks2をメモリカード110へ出力する（ステップS212）。

【0180】メモリカード110の復号処理部1412は、端子1201、インタフェース1423、およびバスBS3を介して {Ks3} Ks2を入力し、セッションキー発生部1418によって発生されたセッションキーKs2によって {Ks3} Ks2を復号して、携帯電話機100で発生されたセッションキーKs3を取得する（ステップS213）。

【0181】セッションキーKs3の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報AC1を確認する（ステップS214）。

【0182】ステップS214においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数制限に制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップS215）。一方、アクセス制限情報AC1によって再生回数制限が制限されていない場合においては、ステップS215はスキップされ、再生回数制限AC1は更新されることなく処理が次のステップ（ステップS216）に進行される。

【0183】また、ライセンス情報保持部1440内にリクエスト曲の当該コンテンツIDが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【0184】ステップS214において、当該再生動作において再生が可能であると判断された場合には、ライセンス情報保持部1440に記録された再生リクエスト曲のライセンス鍵Kcおよび再生期限AC2がバスBS4上に出力される（ステップS216）。

【0185】得られたライセンス鍵Kcと再生期限AC2は、切換スイッチ1444の接点Pdを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点Pdを介して復号処理部1412より受けたセッションキーKs3によってバスBS4から受けたライセンス鍵Kcと再生期限AC2とを暗号化し、{Kc//AC2}Ks3をバスBS3に出力する（ステップS217）。

【0186】バスBS3に出力された暗号化データは、インタフェース1423、端子1202、およびメモリインタフェース1200を介して携帯電話機100に送出される。

【0187】携帯電話機100においては、メモリインタフェース1200を介してバスBS2に伝達される暗号化データ{Kc//AC2}Ks3を復号処理部1212によって復号処理を行ない、ライセンス鍵Kcおよび再生期限AC2を受理する（ステップS218）。復号処理部1212は、ライセンス鍵Kcを復号処理部1214に伝達し、再生期限AC2をバスBS2に出力する。

【0188】コントローラ1106は、バスBS2を介して、再生期限AC2を受理して再生の可否の確認を行なう（ステップS219）。

【0189】ステップS219においては、再生期限AC2によって再生不可と判断される場合には、再生動作は終了される。

【0190】ステップS219において再生可能と判断された場合、コントローラ1106は、メモリインタフェース1200を介してメモリカード110に暗号化コンテンツデータ{Data}Kcを要求する。そうする

と、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Data}Kcを取得し、バスBS3および端子1201を介してメモリインタフェース1200へ出力する（ステップS220）。

【0191】携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して暗号化コンテンツデータ{Data}Kcを取得し、バスBS2を介して暗号化コンテンツデータ{Data}Kcを復号処理部1214へ与える。そして、復号処理部1214は、暗号化コンテンツデータ{Data}Kcを復号処理部1212から出力されたコンテンツ鍵Kcによって復号してコンテンツデータDataを取得する（ステップS221）。

【0192】そして、復号されたコンテンツデータDataは音楽再生部1216へ出力され、音楽再生部1216は、コンテンツデータを再生し、DA変換器1218はデジタル信号をアナログ信号に変換して端子1220へ出力する。そして、スイッチ1222は端子1220を選択して音楽データは端子1224を介してヘッドホン130へ出力されて再生される（ステップS222）。これによって再生動作が終了する。

【0193】図17を参照して、メモリカード110における暗号化コンテンツデータ{Data}Kc、およびライセンス鍵Kc等の記録状況に応じた暗号化コンテンツデータ{Data}Kcおよびライセンス鍵Kc等の配信の例について説明する。図17の(a)を参照して、メモリカード110のデータ領域1415Bには、暗号化コンテンツデータ：{Data(55019930112)}Kc(55019930112)、{Data(55019951013)}Kc(55019951013)、{Data(55019630122)}Kc(55019630122)と、それぞれの関連情報Data-infとが記録されている。また、ライセンス領域1415Aには、コンテンツID：55019930112、トランザクションID：0000000001、ライセンス鍵Kc：AAF53951046FD356ABCC、再生回数制限AC1：00、再生期限AC2：00のライセンスLS1と、コンテンツID：55019951013、トランザクションID：0000000003005、ライセンス鍵Kc：96F539510456AB332C55、再生回数制限AC1：FF、再生期限AC2：00のライセンスLS2とが記録されている。そして、ライセンスLS1については、再生回数制限AC1は「00」であるので、暗号化コンテンツデータ{Data(55019930112)}Kc(55019930112)を再生できない、すなわち、ライセンスがない状態を示している。また、暗号化コンテンツデータ{Data(55019630122)}Kc(5501963012

2) について、コンテンツID、ライセンス鍵Kc、再生回数制限AC1、および再生期限AC2が記録されておらず、ライセンスがない状態を示している。つまり、暗号化コンテンツデータ {Data (55019951013)} Kc (55019951013) に対するライセンスLS2だけが存在し、暗号化コンテンツデータ {Data (55019930112)} Kc (55019930112)、および {Data (55019630122)} Kc (55019630122) に対するライセンスが存在しない状況である。

【0194】図17の(a)に示すメモリカード110の状況において、携帯電話機100のユーザからコンテンツID: 55019930112によって特定される暗号化コンテンツデータ {Data} Kcの配信要求がキー操作部1108を介して入力されると、図9のステップS70～S78が行なわれ、コンテンツID: 55019930112が抽出される(ステップS80)。そして、ステップS82において、「20」回まで再生可能とするライセンスの購入条件ACが入力される。そして、コンテンツID: 55019930112によって特定される暗号化コンテンツデータ {Data} Kcがメモリカード110に記録されているか否かが検索される(ステップS84)。

【0195】この場合、コンテンツID: 55019930112によって特定される暗号化コンテンツデータ {Data} Kcは、メモリカード110に暗号化コンテンツデータ {Data (55019930112)} Kc (55019930112) として記録されているので、図9のステップS86を介してステップS90へ移行する。そして、ステップS90において、ライセンスによって暗号化コンテンツデータ {Data (55019930112)} Kc (55019930112) が再生可能か否かが判断される。この場合、再生回数制限AC1が「00」であるので、暗号化コンテンツデータ {Data (55019930112)} Kc (55019930112) を再生することができない。したがって、ステップS90からステップS94へ移行する。そして、ステップS94においてデータ取得="No"のフラグが立てられた後、ステップS100～ステップS170によって再生回数制限AC1を「20」回とするライセンスだけが配信サーバ30からメモリカード110に配信される。そして、図17の(b)に示すようにライセンスLS1の再生回数制限AC1が「20」と変更される。これによって、ライセンスLS1によって暗号化コンテンツデータ {Data (55019930112)} Kc (55019930112) を再生することができる。

【0196】また、図17の(a)に示すメモリカード110の状況において、携帯電話機100のユーザからコンテンツID: 55012345678によって特定

される暗号化コンテンツデータ {Data} Kcの配信要求がキー操作部1108を介して入力されると、図9のステップS70～S78が行なわれ、コンテンツID: 55012345678が抽出される(ステップS80)。その後、ライセンスの購入条件ACとして、AC1: FF、AC2: 00の再生制限なしが入力される(ステップS82)。そして、コンテンツID: 55012345678によって特定される暗号化コンテンツデータ {Data} Kcがメモリカード110に記録されているか否かが検索される(ステップS84)。この場合、コンテンツID: 55012345678によって特定される暗号化コンテンツデータ {Data} Kcはメモリカード110に記録されていないので、ステップS86からステップS88へ移行し、ステップS88においてデータ取得="Yes"のフラグが立てられる。

【0197】その後、ステップS100～ステップS170が実行され、メモリカード110にコンテンツID: 55012345678、トランザクションID: 000005500345、ライセンス鍵Kc: C6F569510456AB333C4、再生回数制限AC1: FF、再生期限AC2: 00、暗号化コンテンツデータ: {Data (55012345678)} Kc (55012345678)、および関連情報Data D-inf (55012345678) が配信され、かつ、記録される。これによって、メモリカード110は、図17の(c)に示す状態になり、ユーザが配信要求を行なった暗号化コンテンツデータ {Data (55012345678)} Kc (55012345678) の再生が可能となる。

【0198】さらに、図17の(a)に示すメモリカード110の状況において、携帯電話機100のユーザからコンテンツID: 55019630122によって特定される暗号化コンテンツデータ {Data} Kcの配信要求がキー操作部1108を介して入力されると、図9のステップS70～S78が行なわれ、コンテンツID: 55019630122が抽出される(ステップS80)。その後、ライセンスの購入条件ACとして、AC1: FF、AC2: 00の再生制限なしが入力される(ステップS82)。そして、コンテンツID: 55019630122によって特定される暗号化コンテンツデータ {Data} Kcがメモリカード110に記録されているか否かが検索される(ステップS84)。この場合、コンテンツID: 55019630122によって特定される暗号化コンテンツデータ {Data} Kcはメモリカード110に記録されているので、ステップS86からステップS90へ移行する。そして、ステップS90において、ライセンスによって暗号化コンテンツデータ {Data (55019630122)} Kc (55019630122) が再生可能か否かが判断さ

れる。この場合、コンテンツID、ライセンス鍵Kc、再生回数制限AC1、および再生期限ACのいずれもメモリカード110に記録されていないので、暗号化コンテンツデータ{Data(55019630122)}Kc(55019630122)を再生することができない。したがって、ステップS90からステップS94へ移行する。

【0199】そして、ステップS94においてデータ取得="No"のフラグが立てられた後、ステップS100～ステップS170によって再生制限なしとするライセンスだけが配信サーバ30からメモリカード110に配信される。そして、図17の(d)に示すようにコンテンツID:55019630122、トランザクションID:000000550339、ライセンス鍵Kc:F6F53695104AF3323C31、再生回数制限AC1:FF、および再生期限:00がメモリカード110のライセンス領域1415Aに記録される。これによって、暗号化コンテンツデータ{Data(55019630122)}Kc(55019630122)を再生することができる。

【0200】上述したように、携帯電話機100のユーザは、メモリカード110における暗号化コンテンツデータ{Data}Kc、およびライセンス鍵Kc等の記録状況に応じて、携帯電話機100を用いて配信サーバ30から暗号化コンテンツデータ{Data}Kcおよびライセンス鍵Kc等をメモリカード110に受信し、ライセンス鍵Kcによって暗号化コンテンツデータ{Data}Kcを復号し、かつ、再生することができる。

【0201】上記においては、携帯電話機100のユーザが暗号化コンテンツデータ{Data}Kcの配信要求を行なうとき、メモリカード110に記録されている暗号化コンテンツデータ{Data}Kcは、配信サーバ30から受信した暗号化コンテンツデータであるとして説明したが、本発明においては、かかる場合に限らず、配信サーバ30以外から暗号化コンテンツデータ{Data}Kcだけを受信し、メモリカード110に記録した場合も含まれる。

【0202】図18および図19を参照して、配信サーバ30以外の装置から暗号化コンテンツデータ{Data}Kcを受信し、その暗号化コンテンツデータ{Data}Kcをメモリカード110に記録する場合について説明する。

【0203】図18を参照して、コンピュータ140を用いた暗号化コンテンツデータ{Data}Kcの配信について説明する。携帯電話機100にはメモリカード110が着脱可能であり、音楽を再生するためのヘッドホン130が接続されている。そして、携帯電話機100は、通信ケーブル145を介してコンピュータ140と接続されている。

【0204】コンピュータ140は、ハードディスク1

41と、コントローラ142と、外部インタフェース143とを備える。そして、ハードディスク141はバスBS5を介してコントローラ142と接続され、コントローラ142はライセンス保護モジュール143を含む。

【0205】ハードディスク141は、インターネット配信によってコンピュータ140に配信された暗号化コンテンツデータ{Data}KcをバスBS5を介して記憶する。コントローラ142は、携帯電話機100のユーザから通信ケーブル145および外部インタフェース143を介して暗号化コンテンツデータ{Data}Kcの送信要求があると、ハードディスク141から暗号化コンテンツデータ{Data}Kcを読み出し、外部インタフェース143を介して外部へ出力する。

【0206】外部インタフェース143は、携帯電話機100から通信ケーブル145を介してコンピュータ140に入力された信号をコントローラ142に入力するとともに、コントローラ142からの信号を外部へ出力する。

【0207】ライセンス保護モジュール144は、図5に示すデータ処理部310と同じ構成を有し、携帯電話機100に装着されたメモリカード110に暗号化コンテンツデータ{Data}Kcを送信するために、上述したように携帯電話機100およびメモリカード110と公開暗号鍵、セッションキー等のやり取りを行ないながら、暗号化コンテンツデータ{Data}Kcを保護してメモリカード110へ送信するものである。

【0208】インターネット配信によって配信サーバからコンピュータ140に暗号化コンテンツデータ{Data}Kcが配信され、コンピュータ140のハードディスク141にバスBS5を介して暗号化コンテンツデータが記憶されている。

【0209】携帯電話機100のユーザがキー操作部1108から送信要求を入力すると、通信ケーブル145および外部インタフェース143を介して送信要求がコントローラ142に入力される。コントローラ142は、送信要求を受付けると、要求された暗号化コンテンツデータ{Data}KcをバスBS5を介してハードディスク141から読み出し、ライセンス保護モジュール144に入力する。

【0210】ライセンス保護モジュール144は、上述したようにメモリカード110と通信ケーブル145を介して公開暗号鍵、セッションキー等のやり取りを行ない、暗号化コンテンツデータ{Data}Kcをメモリカード110へ送信する。

【0211】送信後、携帯電話機100のユーザは、上述したのと同じ方法によって暗号化コンテンツデータ{Data}Kcのライセンス(コンテンツID、ライセンス鍵Kc、再生回数制限AC1、および再生期限AC2)を配信サーバ30から配信してもらい、暗号化コ

ンテンツデータ {Data} Kcを再生する。

【0212】CDを用いた場合、音楽CDから取得して生成した暗号化コンテンツデータ {Data} Kcは、一旦、ハードディスク141に記録してからメモリカード110へ送信しても良いし、ハードディスク141に送信せずに、直接、メモリカード110へ送信しても良い。

【0213】暗号化コンテンツデータ {Data} Kcは、図19に示すようにメモリカード110を、直接、コンピュータ140に装着してメモリカード110に暗号化コンテンツデータ {Data} Kcを記録しても良い。この場合、コンピュータ140のコントローラ142は、ライセンス保護モジュール144によって、直接、メモリカード110に暗号化コンテンツデータを記録する。

【0214】図19においても、コンピュータ140は、図18に示す場合と同じ方法により暗号化コンテンツデータ {Data} Kcを取得する。

【0215】携帯電話機100が、新たに受信した暗号化コンテンツデータ {Data} Kcに対応するライセンス鍵を含むライセンスの配信要求を配信サーバ30へ行なう場合のフローチャート、および新たに受信した暗号化コンテンツデータ {Data} Kcを再生するフローチャートは、図9～図12、および図15、16に示すフローチャートと同じである。

【0216】再生回数期限AC1および再生期限AC2を、それぞれ、再生回数制限と再生期限として説明したが、再生回数期限AC1は記録装置でのライセンスの扱いに制限を加える制御情報であればよく、また、再生回数はデータ再生端末における再生に対して制限を加えるものであれば何れの制限を行ってもかまわない。

【0217】また、携帯電話機100を暗号化コンテンツデータまたはライセンスの配信を受けるデータ端末装置として説明したが、特に通話機能等は必要なく、ただ、暗号化コンテンツデータまたはライセンスの受信を行えるデータ通信機能を備え、受信したデータを記録できればいかなるデータ端末装置であってもよい。

【0218】さらには、携帯電話機100はコンテンツデータ（音楽データ）を再生する機能を備えているが、必ずしもデータ再生機能を必要とせず、ただ、暗号化コンテンツデータまたはライセンスの受信を行えるデータ通信機能を備え、受信したデータを記録できればいかなるデータ端末装置であってもよい。

【0219】またさらに、着脱可能な記録装置であるメモリカードに暗号化コンテンツデータまたはライセンスを記録するように説明したが、メモリカードに限定するものではない。そして、実施の形態においては、着脱可能な記録装置である必要もない。

【0220】本発明の実施の形態によれば、携帯電話機は、ユーザから暗号化コンテンツデータの配信要求が入

力されると、装着されたメモリカードの記録状況を検索し、その記録状況に応じて必要な暗号化コンテンツデータ、およびライセンス鍵等だけを配信サーバから受信するので、暗号化コンテンツデータ、およびライセンス鍵等が重複してメモリカードに記録されることがない。また、ライセンスを重複して受信することによる無駄な料金を配信サーバへ支払うことを防止できる。さらに、暗号化コンテンツデータを重複して受信することによって無駄な時間が発生するのを防止できる。

【0221】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 ライセンスサーバの構成を示す概略ブロック図である。

【図6】 携帯電話機の構成を示すブロック図である。

【図7】 メモリカードの構成を示すブロック図である。

【図8】 メモリカードの記録状態を説明するための概念図である。

【図9】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図10】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図11】 図1に示すデータ配信システムにおける配信動作を説明するための第3のフローチャートである。

【図12】 図1に示すデータ配信システムにおける配信動作を説明するための第4のフローチャートである。

【図13】 配信サーバから携帯電話機に送信されたコンテンツメニューを携帯電話機の表示部に表示した状態を示す図である。

【図14】 メモリカードのメモリにおけるデータフォーマットである。

【図15】 携帯電話機における再生動作を説明するための第1のフローチャートである。

【図16】 携帯電話機における再生動作を説明するための第2のフローチャートである。

【図17】 メモリカードの記録状況に応じた暗号化コンテンツデータおよびライセンスの配信例を説明する図

である。

【図18】 コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための概略図である。

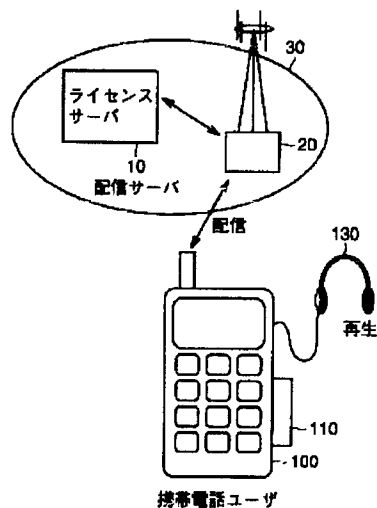
【図19】 コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための他の概略図である。

【符号の説明】

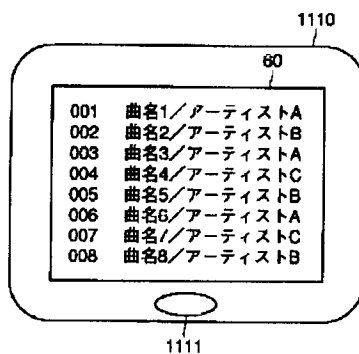
10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、60 コンテンツメニュー、100 携帯電話機、110 メモリカード、130 ヘッドホン、140 コンピュータ、141 ハードディスク、142、1106、1420 コントローラ、143 外部インタフェース、144 ライセンス保護モジュール、145 通信ケーブル、302 課金データベース、304 情報データベース、306 CRLデータベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1206、1212、1214、1404、1408、1412、1422 復号処理部、313 認証鍵保

持部、315 配信制御部、316、1210、1418 セッションキー発生部、318、326、328、1208、1406、1410 暗号処理部、350 通信装置、1102 アンテナ、1104 送受信部、1108 キー操作部、1110 ディスプレイ、1111 移行部、1112 音声再生部、1113、1218 DA変換器、1114、1201、1220、1224 端子、1115 マイク、1116 AD変換器、1117 音声符号化部、1200 メモリインタフェース、1202、1400 認証データ保持部、1204 Kp1保持部、1216 音楽再生部、1222 スイッチ、1402 Kmc1保持部、1414 KPma保持部、1415 メモリ、1415A CR領域、1415B データ領域、1416 KPm1保持部、1421 Km1保持部、1423 インタフェース、1424 Header、1440 ライセンス情報保持部、1442、1444、1446 切換スイッチ。

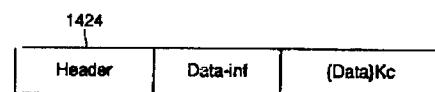
【図1】



【図13】



【図14】



【図4】

| 名称 | 属性 | 保持/発生箇所 | 機能・特徴 |
|------|-----------------|---------|--|
| Ks1 | 共通鍵 | 配信サーバ | 配信セッション毎に発生 |
| Ks2 | | メモリカード | 配信/再生セッション毎に発生 |
| Ks3 | | 携帯電話機 | 再生セッション毎に発生 |
| Km | 秘密復号鍵 | メモリカード | メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能 |
| KPm | 公開暗号鍵 (非対称鍵) | メモリカード | メモリカードごとに固有の暗号鍵 |
| KPma | 公開認証鍵 | 配信サーバ | 配信システム全体で共通。 |

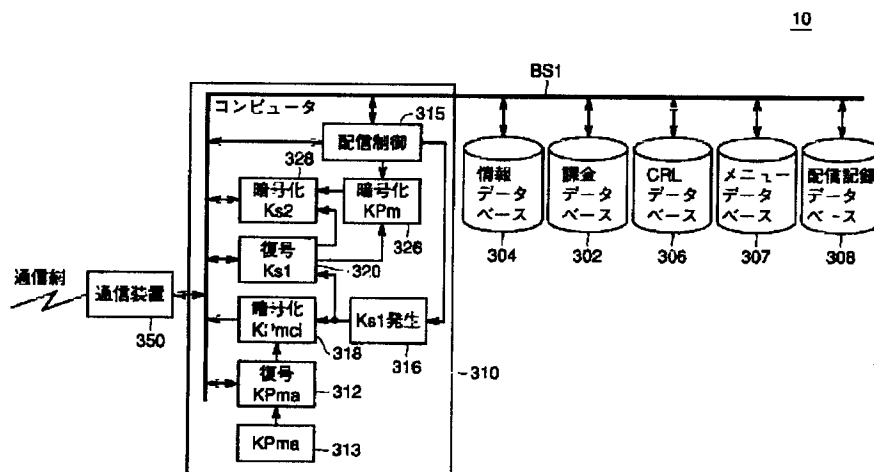
【図2】

| 名称 | 属性 | 保持/発生箇所 | 機能・特徴 |
|------------|-------------|---------|--|
| Data | コンテンツデータ | 配信サーバ | 例：音楽データ、アップデータプログラム |
| Kc | ライセンス鍵 | | 暗号化コンテンツデータの復号鍵 |
| {Data}Kc | 暗号化コンテンツデータ | | 共通鍵Kcで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバより配布。 |
| Data-Inf | 付加情報 | | 例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報 |
| コンテンツID | コンテンツに関する情報 | | コンテンツデータDataを識別するコード |
| ライセンスID | ライセンスに関する情報 | | ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可) |
| トランザクションID | ライセンス固有 | | 記帳を特定するための管理コード |
| AC | ライセンス購入条件 | | 利用者側から指定(例：ライセンス数、機能限定等) |
| AC1 | アクセス制限情報 | | メモリのアクセスに対する制限(例：再生可能回数) |
| AC2 | 再生回路制御情報 | | コンテンツ再生回路(携帯電話機)における制御情報 (例：再生可否) |

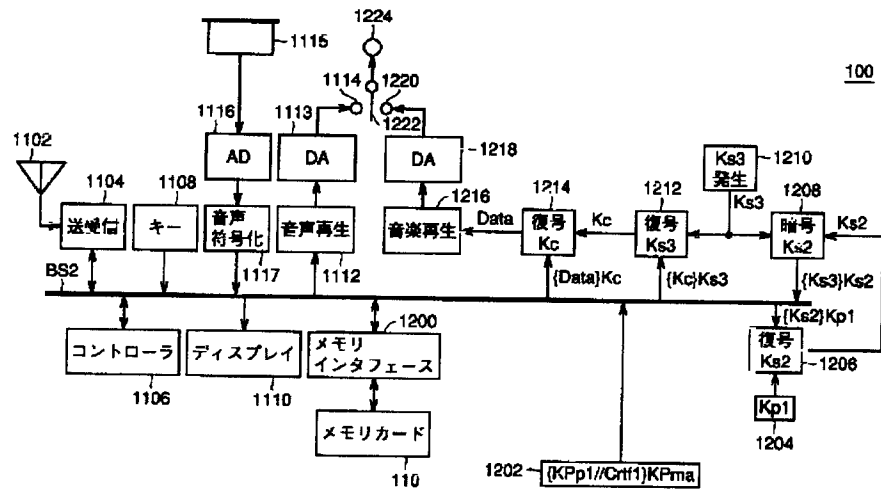
【図3】

| 名称 | 属性 | 保持/発生箇所 | 機能・特徴 |
|---------|-----------------|-----------------|--|
| C:IL | 禁止クラスリスト関連情報 | 配信サーバ メモリカード | 禁止クラスリストの対象クラスデータ |
| CHL_dat | | 配信サーバ | 禁止クラスリストのバージョン更新のための情報 |
| CRL_ver | | メモリカード | 禁止クラスリストのバージョン情報 |
| KPpn | 公開暗号鍵 (非対称鍵) | 携帯電話機 | Kpnにて復号可能。 {KPpn/Crtfn}KPmaの形式で出荷時に記録 *携帯電話機の種類nごとに異なる。 |
| KPmcl | 公開暗号鍵 (非対称鍵) | メモリカード | Kmclにて復号可能。 {KPmcl/Cmcl}KPmaの形式で出荷時に記録 *メモリカードの種類iごとに異なる。 |
| Kpn | 秘密復号鍵 | 携帯電話機 | コンテンツ再生回路(携帯電話機)固有の復号鍵 *携帯電話機の種類nごとに異なる。 |
| Kmcl | 秘密復号鍵 | メモリカード | メモリカード固有の復号鍵 *メモリカードの種類iごとに異なる。 |
| Crtfn | クラス証明書 | 携帯電話機 | コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPpn/Crtfn}KPmaの形式で出荷時に記録 *携帯電話機のクラスnごとに異なる。 |
| Cmcl | | メモリカード | メモリカードのクラス証明書。認証機能を有する。 {KPmcl/Cmcl}KPmaの形式で出荷時に記録 *メモリカードのクラスiごとに異なる。 |

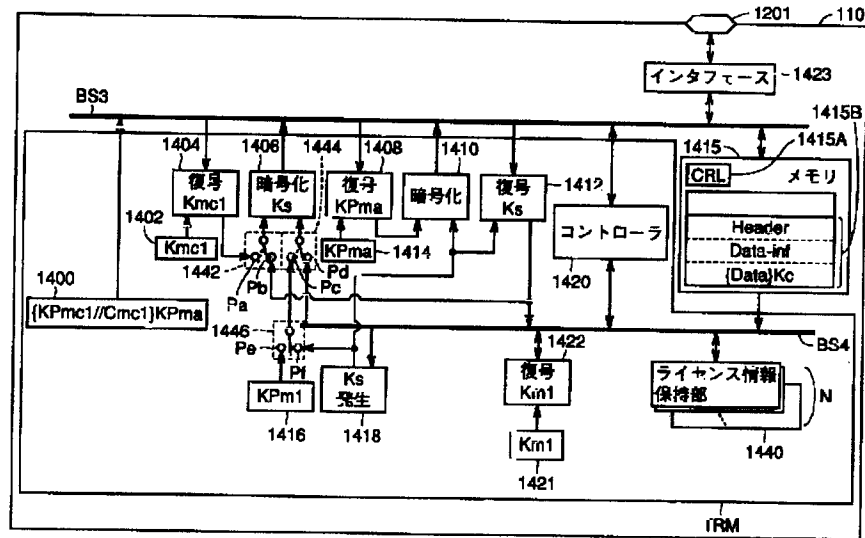
【図5】



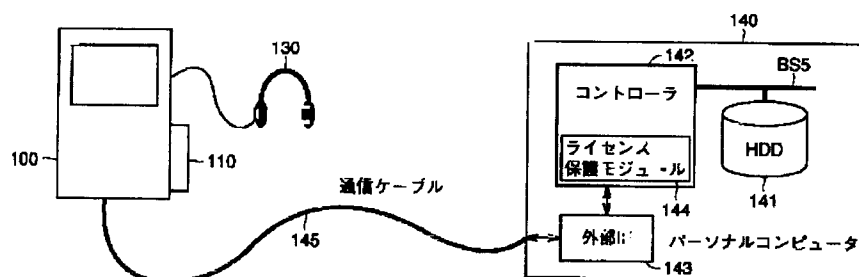
【図6】



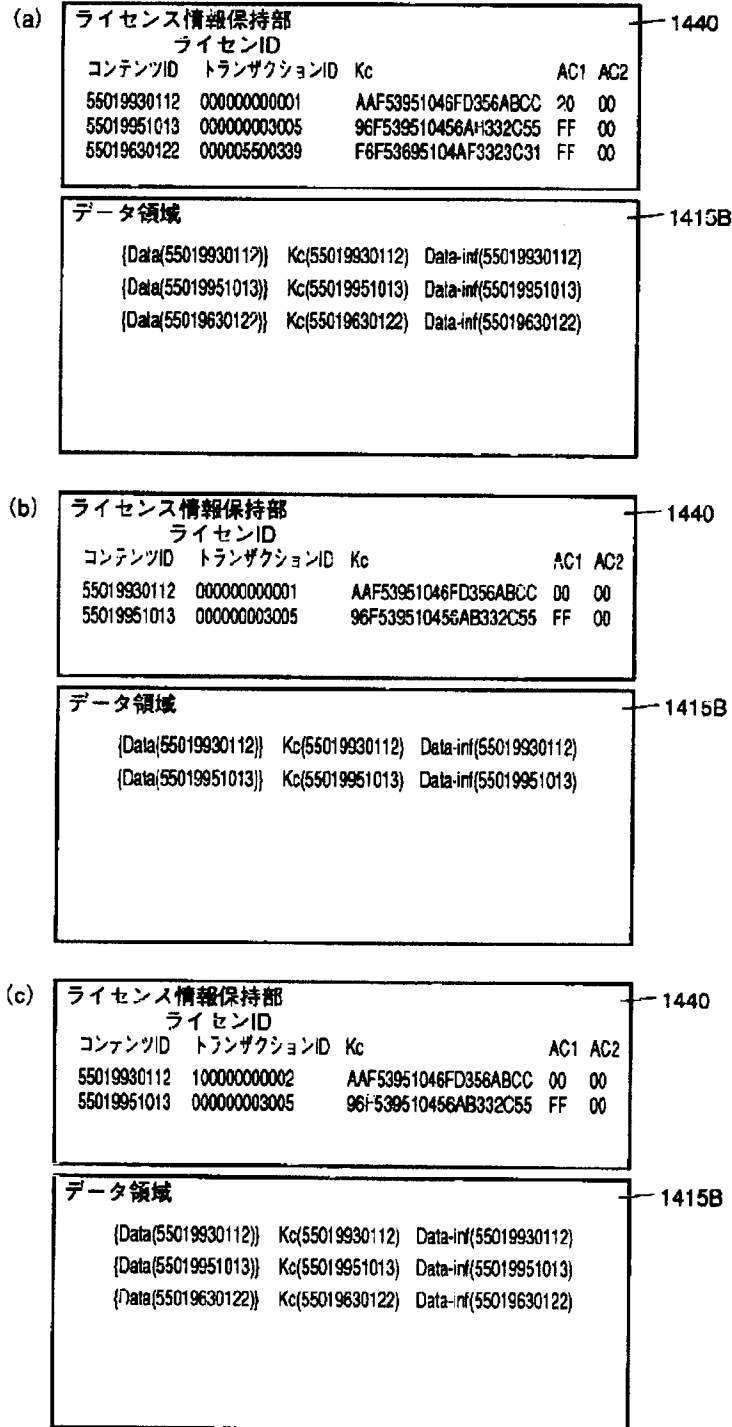
【図7】



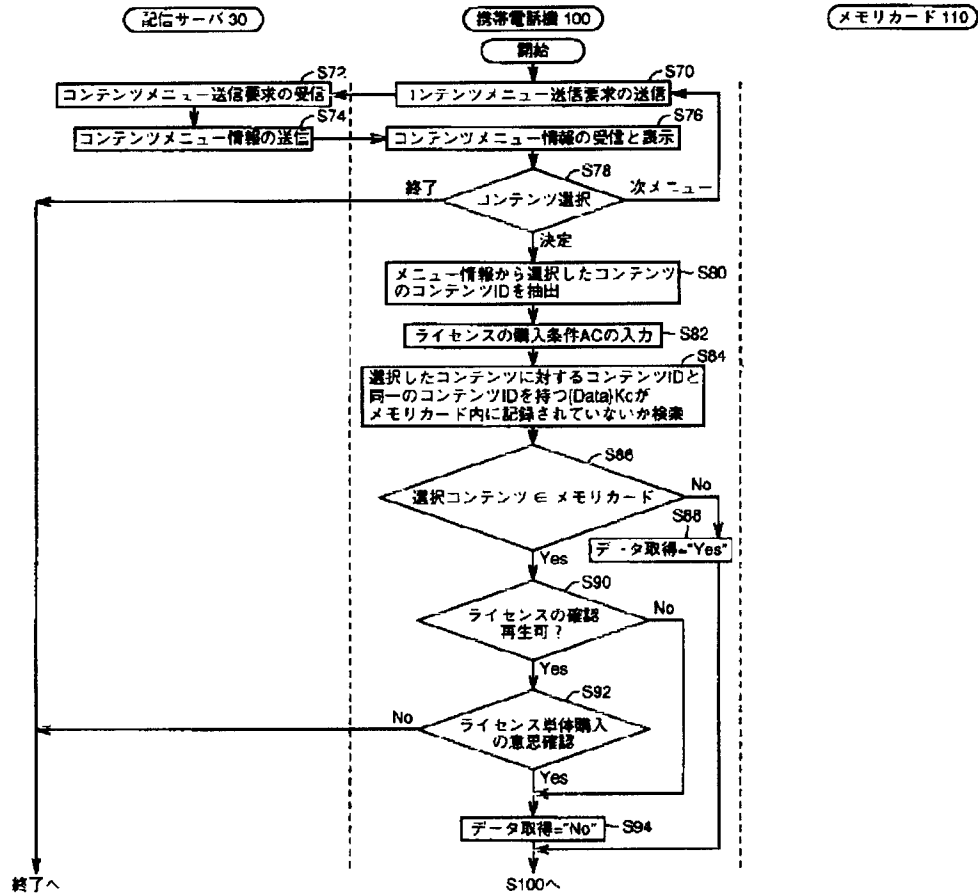
【図18】



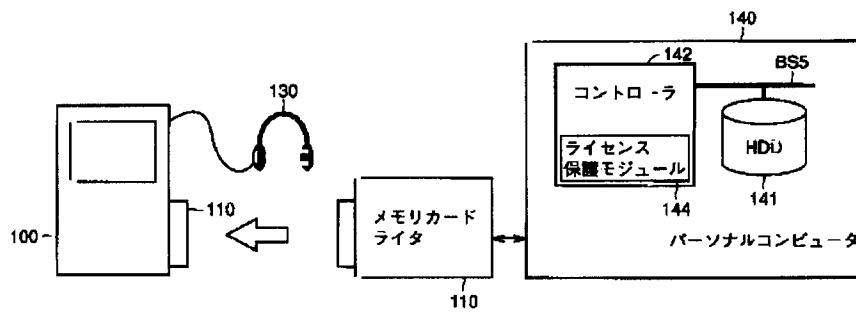
【図8】



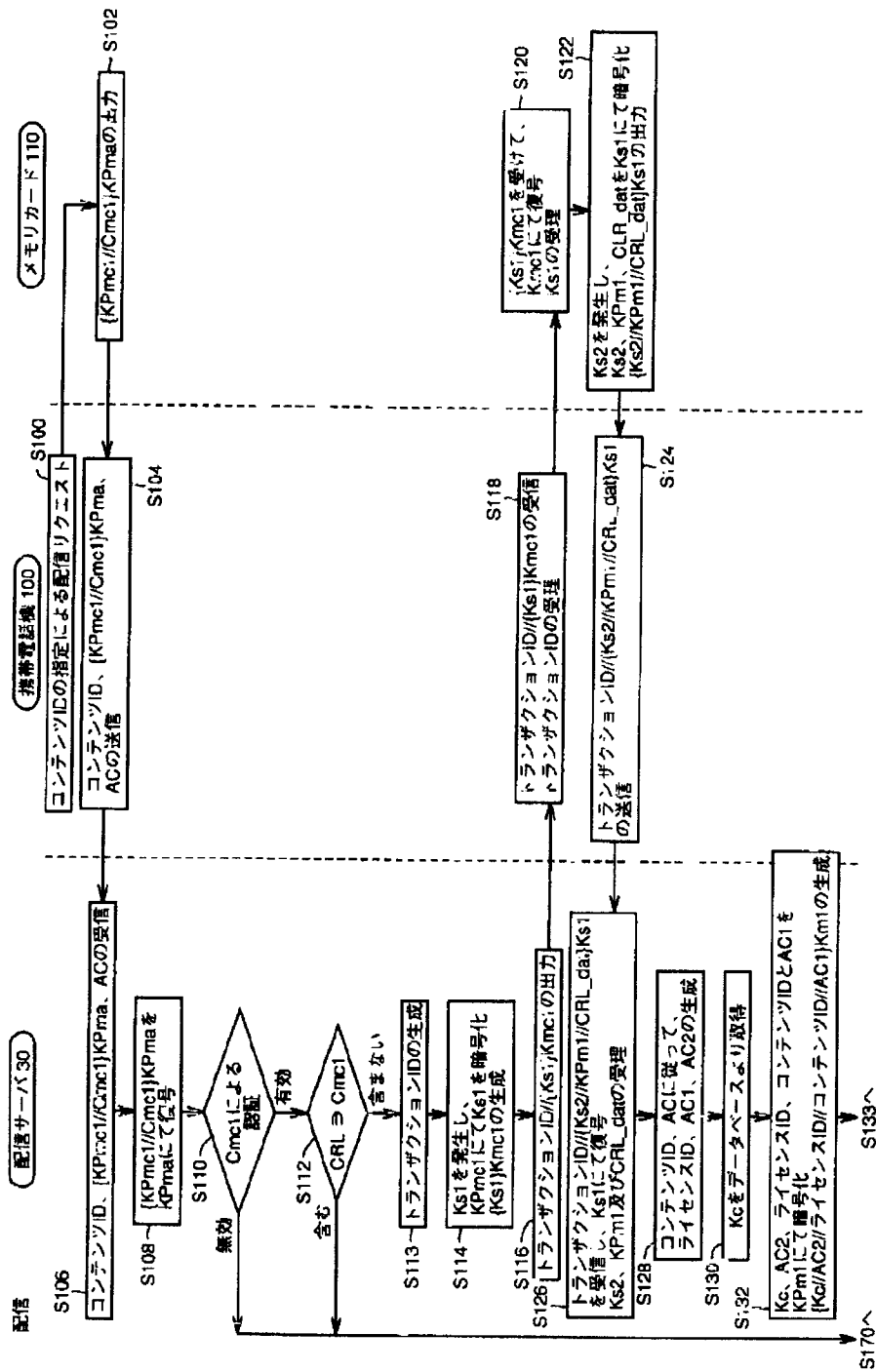
【図9】



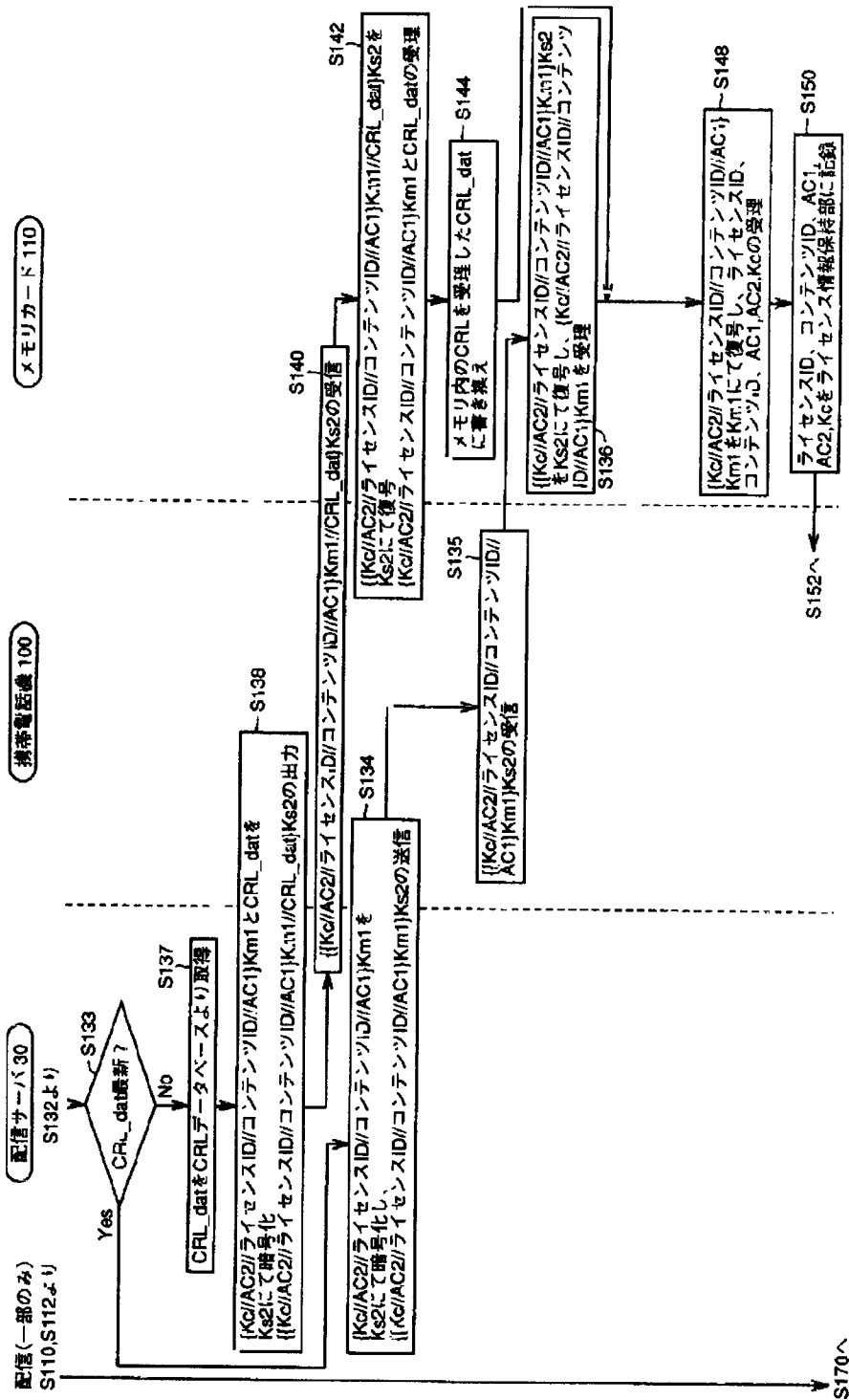
【図19】



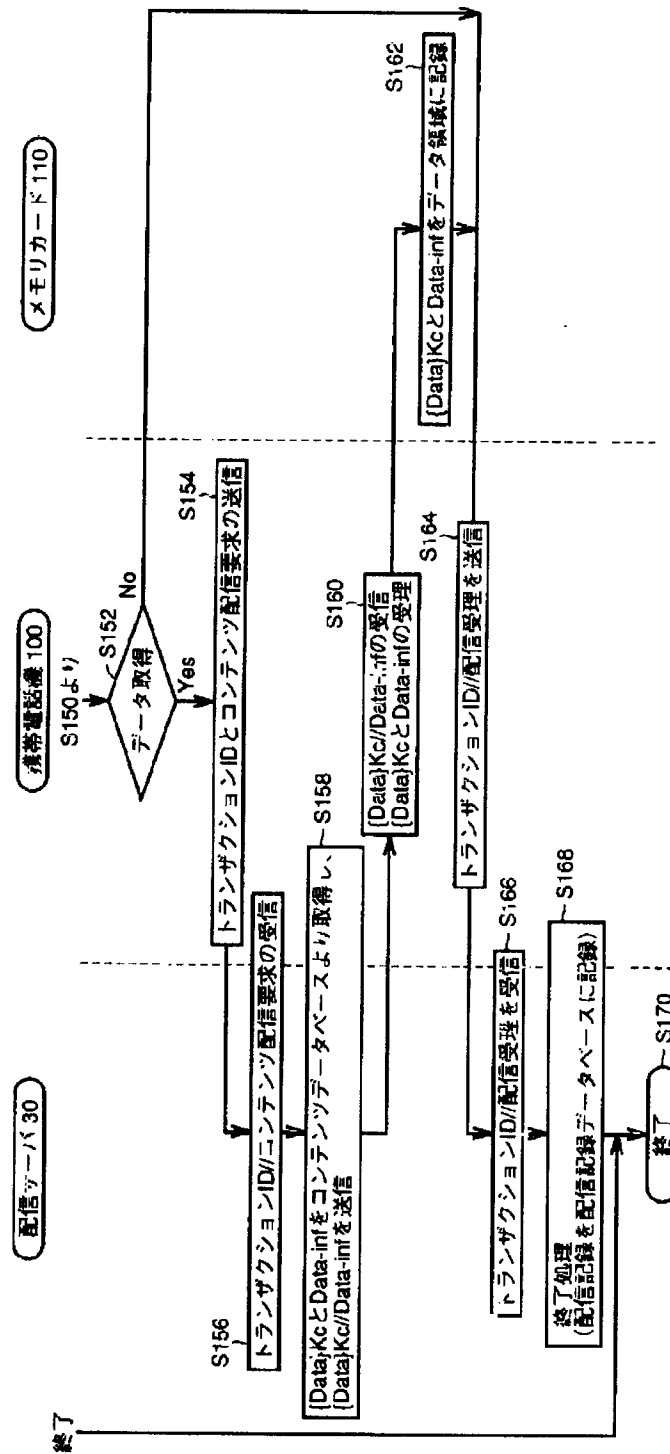
【図10】



【図11】



【図 12】



【図15】

